IN THE CLAIMS

1. (Currently amended) A method comprising:

receiving a call request over a packet switched network at a first gateway that is located between the packet switched network and a circuit switched network;

comparing a phone number included in the call request with entries in a local dial plan located at the first gateway;

sending one or more signals from the first gateway to a source endpoint when the phone number included in the request matches one of the entries in the local dial plan, the signals directing the source endpoint to encrypt media packets for the requested call using a protocol for encrypting real-time media;

receiving the encrypted media packets from the source endpoint responsive to sending the signals;

when a transfer path for the requested call includes a leg traversing the circuit switched network, determining whether a remote second gateway that is located on the [[a]] transfer path ~~for the encrypted media packets that are received according to the signals~~ and ~~that is located~~ between the circuit switched network and the same or another packet switched network is configured for end-to-end secure transport ~~when the requested call is to be transferred using the circuit switched network~~;

establishing an Internet Protocol (IP) link that traverses ~~over~~ the circuit switched network when the second gateway is configured for end-to-end secure transport, the IP link extending from the first gateway to the second gateway ~~when the second gateway is configured for end-to-end secure transport~~; ~~and~~

reformatting the encrypted media packets for transport over the IP link when the second gateway is configured for end-to-end secure transport, said reformatting occurring without decrypting an encrypted payload attached to the encrypted media packets; and

transferring the reformatted encrypted media packets over the established IP link.

2. (Currently amended) A method according to claim 1 further including:

decrypting the payload ~~the encrypted media packets~~ locally at the first gateway when the remote second gateway is not configured for end-to-end secure transport;

formatting media included in the encrypted media packets into a Public Switched Telephone Network ~~Packet Switched Telephone Network~~ (PSTN) format when the remote second gateway is not configured for end-to-end secure transport; and

transferring the formatted media over the circuit switched network for re-encryption at the remote second gateway.

3. (Previously presented) The method according to claim 1 including establishing a data channel over the circuit switched network and using a Point to Point Protocol over the data channel to establish the IP link.

4. (Previously presented) A method according to claim 3 including establishing the data channel over an Integrated Services Digital Network (ISDN) channel of the circuit switched network.

5. (Cancelled)

6. (Cancelled)

7. (Currently amended) A method according to claim 1 including:

authenticating the second gateway;

sending a first encrypted key associated with the source endpoint over the circuit switched network to the authenticated second gateway;

receiving a second encrypted key over the circuit switched network from the authenticated second gateway;

decrypting the second key and forwarding the decrypted second key over the packet switched network to the source endpoint;

encrypting the payload ~~media packets~~ at the source endpoint using the first key according to the signals~~, the encrypted media packets directed to a destination endpoint~~; and

decrypting the payload ~~IP packets received~~ at the source endpoint using the second key.

8. (Currently amended) A method according to claim 1 including encrypting the payload ~~media packets~~ only once, said encryption occurring at the source endpoint, and

decrypting the payload ~~media packets~~ only once, said decryption occurring at a destination ~~receiving second~~ endpoint.

9. (Currently amended) A method according to claim 1 including:

encrypting the payload ~~media packets~~ using a Secure Real-time Transport Protocol (SRTP);

establishing a Point to Point Protocol (PPP) connection over an Integrated Services Digital Network(ISDN) channel in the circuit switched network; and

sending the SRTP encrypted payload ~~IP media packets~~ over the PPP connection.

10. (Currently amended) A network processing device, comprising:

a processor configured to establish an Internet Protocol (IP) link for transferring received IP packets ~~encrypted IP packet payloads~~ over a circuit switched network, the IP link extending across the circuit switched network and between the network processing device and a remote gateway that is located between a packet switched network and the same or another circuit switched network;

the processor configured to identify one or more IP headers included in the received IP packets, to remove the IP headers while preserving encryption on one or more Secure Real-time Transport Protocol (SRTP) headers and a corresponding payload, to locally generate one or more new IP headers, to attach the generated IP headers to the encrypted SRTP headers and the encrypted corresponding payload, to forward the IP packets having the locally generated IP headers, the encrypted SRTP headers and the encrypted corresponding payload over the IP link;

~~the processor forwarding packets having an encrypted IP packet payload~~ wherein the IP packets are forwarded over the IP link without decrypting the payload ~~encrypted IP packet payload~~.

11. (Cancelled)

12. (Currently amended) A network processing device according to claim 10 wherein the processor compresses the forwarded IP packets using a first data compression codec having greater data compression capability than a second data compression codec used by the processor for other traffic that is decrypted before forwarding over a data link in the circuit switched network.

13. (Currently amended) A network processing device according to claim 10 including a memory containing a dial plan for identifying phone numbers that can be transferred between the packet switched network and the circuit switched network without decrypting the received IP packets ~~decrypting the encrypted IP packet payload~~.

14. (Previously presented) A network processing device according to claim 10 including memory for storing a shared key shared with the remote gateway, the processor receiving a first key from a first endpoint, encrypting the first key using the shared key and sending the encrypted first key to the remote gateway.

15. (Previously presented) A network processing device according to claim 14 wherein the processor receives a second encrypted key from the remote gateway, the processor decrypting the second encrypted key using the shared key and then forwarding the second decrypted key to the first endpoint.

16. (Currently amended) A network processing device according to claim 10 wherein the processor conducts a Point to Point Protocol over an Integrated Services Digital Network (ISDN) channel for establishing the IP link over the circuit switched network ~~and then forwards Secure Real-time Transport Protocol (SRTP) encrypted IP packet payloads over the IP link~~.

17. (Previously presented) A method for transporting encrypted media, comprising:

receiving a call request over a packet switched network at a first gateway that is located between the packet switched network and a circuit switched network;

determining whether a second on-path gateway includes a capability for end-to-end secure real-time transport in response to receiving the call request;

transferring the encrypted media packets over an Internet Protocol (IP) connection that traverses the circuit switched network and extends between the first and second gateways when the second gateway includes the capability for end-to-end secure real-time transport; and

converting the received encrypted media packets to a Publicly Switched Telephone Network (PSTN) format for transmission across a different connection that also traverses the circuit switched network when the second gateway does not include the capability for end-to-end secure real-time transport.

18. (Previously presented) The method according to claim 17 including:

authenticating the call request with the second gateway;

conducting Point-to-Point Protocol (PPP) sessions with the second gateway when the second gateway is authenticated; and

exchanging encryption keys with the second gateway during the PPP session.

19. (Previously presented) The method according to claim 18 including:

encrypting the encryption keys using keys shared with the second gateway; and

sending the encrypted encryption keys to the second gateway.

20. (Currently amended) A method comprising: ~~An apparatus, comprising:~~

receiving packets from a packet switched network;

establishing an Internet Protocol (IP) link for transferring received packets over a circuit switched network;

identifying one or more addressing headers included in the received packets;

removing the addressing headers while preserving encryption on one or more Secure Real-time Transport Protocol (SRTP) headers and a corresponding payload;

attaching new addressing headers to the encrypted SRTP headers and the encrypted corresponding payload;

forwarding the packets having the new addressing headers, the encrypted SRTP headers and the encrypted corresponding payload over the IP link; and

wherein the packets are forwarded over the IP link without decrypting the payload.

~~one or more processors; and~~

~~a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to:~~

~~receive media packets over a packet switched network at a first gateway that is located between the packet switched network and a circuit switched network, the media packets encrypted with a protocol for encrypting real-time media;~~

~~determine whether a remote second gateway is configured for end-to-end secure real-time transport before establishing an Internet Protocol (IP) connection over the circuit switched network and to the remote second gateway; and~~

~~transfer the encrypted media packets over the established IP connection when the remote second gateway is configured for end-to-end secure real-time transport.~~

21. (Currently amended) The method ~~apparatus~~ of claim 20 further comprising ~~wherein the processors are further operable to~~:

comparing ~~compare~~ a phone number included in a call request with a dial plan, the call request being associated with the packets and received before the packets ~~for the media packets with a dial plan~~; and

sending ~~send~~ a signal that is configured to cause ~~that causes~~ an originating ~~a source~~ endpoint to perform encryption using SRTP ~~for the media packets to encrypt the media packets with the protocol~~ when the phone number corresponds with the dial plan.

22. (Currently amended) The method ~~apparatus~~ of claim 20 wherein the ~~encrypted media~~ packets include voice data such that the voice data is securely transported across both the circuit switched network and the packet switched network without intermediary decryption.

23. (Cancelled)

24. (Currently amended) The network processing device according to claim 10 where the processor is further configured to:

receive a pre-configuring out-of-band communication that provides a secret that is shared with the remote gateway;

receive a first key sent from a calling endpoint and usable for decrypting the IP packets ~~encrypted IP packet payload~~;

encrypt the first key using the secret;

send the encrypted first key to the remote gateway;

receive a second key that corresponds to a value stored on a called endpoint and that is encrypted by the remote gateway using the secret;

decrypt the received encrypted second key using the secret; and

send the decrypted second key to the calling endpoint.

25. (Currently amended) A system, comprising:

means for receiving packets from a packet switched network;

means for establishing an Internet Protocol (IP) link for transferring received packets over a circuit switched network;

means for identifying one or more addressing headers included in the received packets;

means for removing the addressing headers while preserving encryption on one or more secure real time protocol headers and a corresponding payload;

means for attaching new addressing headers to the encrypted secure real time protocol headers and the encrypted corresponding payload; and

means for forwarding the packets having the new addressing headers, the encrypted secure real time protocol headers and the encrypted corresponding payload over the IP link;

wherein the packets are forwarded over the IP link without decrypting the payload.

~~first and second network devices, at least one of the first and second network devices located between a packet switched network and a circuit switched network;~~

~~the first network device to receive encrypted media packets from a source endpoint; and~~

~~the first network device to transfer the encrypted media packets over a connection extending through the circuit switched network and extending to the second network device for forwarding to a destination endpoint without decryption by the second network device;~~

~~wherein the encrypted media packets are sent from the source endpoint to the destination endpoint over a call path that extends across both the packet switched network and the circuit switched network without decryption by any intermediary devices located on the call path.~~

26. (Currently amended) The system of claim 25 wherein the ~~encrypted media~~ packets represent video to be played out at the destination endpoint.

27. (Currently amended) The system of claim 25 wherein the new addressing headers are attached at a first gateway located between a circuit switched network and a packet switched network and the packets are forwarded to a second gateway located between the same or another circuit switched network and the same or another packet switched network ~~both the first and second network devices are gateways located between the circuit switched network and the packet switched network~~.

28. (Cancelled)

29. (Currently amended) The system of claim 27 [[28]] wherein the first gateway ~~network device~~ is configured to determine whether the second gateway ~~third network device~~ supports ~~is capable of~~ an End-to-End Secure Real-time Transport Protocol (EE-SRTP) protocol by accessing a dial plan stored locally on the first gateway ~~network device~~.